**MATH 521A: Abstract Algebra**
Preparation for Exam 1

1. Prove that $S = \mathbb{N} \cup \{\pi\}$ is well-ordered.

2. Let $S$ be a set with a well-ordering $<$, and for each $x \in S$ the proposition $P(x)$ may be true or false. Suppose that $c \in S$ is the smallest counterexample, i.e. $P(c)$ is false, but for all $x \in S$ with $x < c$, $P(x)$ is true. Suppose that with these hypotheses we are able to derive a contradiction. Prove that $P(x)$ holds for all $x \in S$, using the well-ordering of $S$.

3. Let $m \in \mathbb{N}$. Use the division algorithm to prove that there is no integer $n$ with $m < n < m + 1$.

4. Let $p \in \mathbb{N}$ be irreducible, with $p > 4$. Use the Division Algorithm to prove that $p$ is of the form $6k + 1$ or $6k + 5$ for some integer $k$.

5. Prove the following variant of the division algorithm: Let $a, b$ be integers with $b > 0$. then there exist (not necessarily unique) integers $q, r$ such that $a = bq + r$ and $-1 \leq r \leq b - 2$.

6. Let $a, b, c \in \mathbb{Z}$. Suppose that $a|b$ and $a|c$. Prove that $a|(bx + cy)$ for any $x, y \in \mathbb{Z}$.

7. Prove the Euclidean Algorithm: Let $a, b, q, r \in \mathbb{Z}$ with $b > 0$ and $a = bq + r$. Prove that $\gcd(a, b) = \gcd(b, r)$.

8. Use the extended Euclidean Algorithm to find $\gcd(119, 189)$ and to find $x, y \in \mathbb{Z}$ with $119x + 189y = \gcd(119, 189)$.

9. Prove Theorem 1.4 in the text: Let $a, b, c \in \mathbb{Z}$, with $a|bc$ and $\gcd(a, b) = 1$. Prove that $a|c$.

10. Let $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$. Without using the FTA, prove that $\gcd(a^2, b) = 1$.

11. Let $a, b, c, d \in \mathbb{Z}$ with $a|c$, $b|c$, and $\gcd(a, b) = d$. Without using the FTA, prove that $ab|cd$.

12. Find all perfect squares dividing 144.

13. Let $a, b, c \in \mathbb{Z}$ with $ab = c^2$ and $\gcd(a, b) = 1$. Prove that $a, b$ are perfect squares.

14. Let $p \in \mathbb{N}$ be irreducible with $p \neq 3$. Prove that $p^2 + 2$ is reducible.

15. Apply the Miller-Rabin test to $n = 63$ and $a = 7$, and interpret the result.